IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

JERIKA BARNES JENKINS, MICHELLE SIMMONS, RAYOMI WOODS, KAYOMI WILLIAMS, and KAYOMI WILLIAMS on behalf of L.S., A MINOR, ON BEHALF OF THEMSELVES AND ALL OTHERS SIMILARLY SITUATED, *Plaintiffs*, v. BETTY JEAN KERR PEOPLE'S HEALTH CENTERS, *Defendant*.	)	Case No. Judge: ***JURY TRIAL DEMANDED***

CLASS ACTION COMPLAINT

1. Plaintiffs, JERIKA BARNES JENKINS, MICHELLE SIMMONS, RAYOMI WOODS, KAYOMI WILLIAMS, and KAYOMI WILLIAMS on behalf of L.S., a minor, individually, and on behalf of all others similarly situated, bring this action against Defendant, BETTY JEAN KERR PEOPLE'S HEALTH CENTERS ("PHC" or "Defendant") to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record:

JURISDICTION AND VENUE

2. This Court has jurisdiction over this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d). There are at least 100 members in the proposed class, the aggregated claims of the individual Class Members exceed the sum or value of $5,000,000.00 exclusive of interest and costs, and members of the Proposed Class (such as named Plaintiff Jenkins) are citizens of states

different from Defendant. In addition, this Court has federal question subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because the Plaintiffs assert claims that necessarily raise substantial disputed federal issues under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Federal Trade Commission Act (15 U.S.C. § 45) and the Gramm-Leach-Bliley Act (15 U.S.C. § 6801). *See, e.g.*, *infra* at ¶ 53.

3. Defendant has sufficient minimum contacts in Missouri, as it is organized as a nonprofit corporation under the laws of the State of Missouri, and conducts the majority (if not all) of its business in the State of Missouri, thus rendering the exercise of jurisdiction by this Court proper and necessary.

4. Venue is proper in this District under 28 U.S.C. § 1391 because a substantial part of the events and omissions giving rise to these claims occurred in this District.

NATURE OF THE ACTION

5. This class action arises out of the recent ransomware attack at PHC's medical facilities that disrupted operations by, among other things, blocking access to PHC's computer systems and data, including the highly sensitive patient medical records of PHC patients (the "Ransomware Attack"). As a result of the Ransomware Attack, Plaintiffs and class members suffered ascertainable losses in the form of disruption of medical services, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack. In addition, Plaintiffs' and class members' sensitive personal information—which was entrusted to PHC, its officials and agents—was compromised and unlawfully accessed due to the Ransomware Attack. Information compromised in the Ransomware Attack includes patient names, dates of birth, Social Security numbers, limited clinical data, pharmacy data, insurance information, dental x-rays, other protected health information as defined by HIPAA, and additional personally identifiable information ("PII")

and protected health information ("PHI") that Defendant PHC collected and maintained (collectively the "Private Information").

6. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of class members' Private Information that it collected and maintained.

7. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant PHC's computer network in a condition vulnerable to cyberattacks of the type that cause actual disruption to Plaintiffs' and class members' medical care and treatment. As a result of the Ransomware Attack, Plaintiffs' and class members' Private Information was seized and held hostage by computer hackers for 'ransom', and ultimately disclosed to other unknown thieves. Upon information and belief, the mechanism of the ransomware and potential for improper disclosure of Plaintiffs' and class members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

8. Because of the Ransomware Attack, Plaintiffs and class members had their medical care and treatment as well as their daily lives disrupted. As a consequence of the ransomware locking down the medical records of Plaintiffs and class members, Plaintiffs and class members had to, among other things, forego medical care and treatment or had to seek alternative care and treatment.

9. What's more, aside from having their lives disrupted, Plaintiffs' and Class Members' identities are now at risk because of Defendant's conduct since the Private Information that Defendant PHC collected and maintained is now in the hands of data thieves.

10. Armed with the Private Information accessed in the Ransomware Attack, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in class members' names, taking out loans in class members' names, using class members' names to obtain medical

services, using class members' health information to target other phishing and hacking intrusions based on their individual health needs, using class members' information to obtain government benefits, filing fraudulent tax returns using class members' information, obtaining driver's licenses in class members' names but with another person's photograph, and giving false information to police during an arrest.

11. As a further result of the Ransomware Attack, Plaintiffs and class members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and class members must now and in the future closely monitor their financial accounts to guard against identity theft.

12. Plaintiffs and class members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

13. By their Complaint, Plaintiffs seeks to remedy these harms on behalf of themselves and all similarly-situated individuals whose Private Information was accessed or ransomed during the Ransomware Attack.

14. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

15. Accordingly, Plaintiffs bring this action against Defendant PHC seeking redress for PHC's unlawful conduct, and asserting claims for: (i) breach of express contract and (ii) breach of implied contract; and (iii) violations of the Missouri Merchandising Practices Act.

PARTIES

16. Plaintiff, JERIKA BARNES JENKINS, is and at all times mentioned herein was, an individual citizen of the State of Florida residing in the City of Jacksonville.

17. Plaintiff, MICHELLE SIMMONS, is and at all times mentioned herein was, an individual citizen of the State of Missouri residing in the City of St. Louis.

18. Plaintiff, RAYOMI WOODS, is and at all times mentioned herein was, an individual citizen of the State of Missouri residing in the City of St. Louis.

19. Plaintiff, KAYOMI WILLIAMS, is and at all times mentioned herein was, an individual citizen of the State of Missouri residing in the City of St. Louis.

20. Plaintiff, L.S., a minor, through her parent and legal guardian, KAYOMI WILLIAMS, is and at all times mentioned herein was, an individual citizen of the State of Missouri residing in the City of St. Louis.

21. Defendant PHC is a Missouri nonprofit corporation with its principal place of business at 5701 Delmar Blvd., St. Louis, MO 63112.

DEFENDANT'S BUSINESS

22. Defendant PHC is in the business of providing healthcare to the St. Louis metropolitan area.

23. Services and subspecialties offered by Defendant include, but are not limited to, providing comprehensive primary health care, such as pediatrics, internal medicine, OB/GYN, dental, mammography, behavioral health, pharmacy, radiology, podiatry and laboratory services.

24. In the ordinary course of receiving treatment and health care services from Defendant PHC, patients are required to provide Defendant with sensitive, personal and private information such as:

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;
- Social Security number;

- Information relating to individual medical history;
- Insurance information and coverage;
- Information concerning an individual's doctor, nurse or other medical providers;
- Photo identification;
- Employer information, and;
- Other information that may be deemed necessary to provide care.

25. Defendant PHC also gathers certain medical information about patients and creates records of the care it provides to them.

26. Additionally, Defendant PHC may receive private and personal information from other individuals and/or organizations that are part of a patient's "circle of care", such as referring physicians, patients' other doctors, patient's health plan(s), close friends, and/or family members.

27. All of Defendant's employees, staff, entities, clinics, sites, and locations may share patient information with each other for various purposes, as disclosed in the Notice of Privacy Practices (the "Privacy Notice").[1] The current privacy notice was last revised on November 4, 2013.

28. The Privacy Notice is provided to every patient upon request and is posted on Defendant's websites.

29. Because of the highly sensitive and personal nature of the information Defendant acquires and stores with respect to its patients, PHC promises to: (1) maintain "the privacy of your individually identifiable health information ("IIHI")"; (2) notify a patient of a "breach of any of your unsecured Protected Health Information within 60 days"; (3) "provide you with this notice of our legal duties and the privacy practices that we maintain in our Health Center concerning your IIHI";

[1] https://peoplesfamilystl.org/wp-content/uploads/2017/06/2000-12-Notice-of-Privacy-Practices.pdf

(4) abide by the legal requirement "to maintain the confidentiality of health information that identifies you," and; (5) follow the terms of the Notice of Privacy Practices that PHC has in effect at the time.[2]

30. PHC's Privacy Notice also explicitly affirms the "Automatic Presumption" that "any impermissible use or access is presumed to be a breach."[3]

31. PHC makes similar promises in its "Patients' Rights and Responsibilities," in which it promises the confidentiality of Health Information, and that patients have the right "to have their health care information protected."[4]

32. In addition to the promises made to patients, PHC also makes contractual promises to health care providers who wish to be credentialed by PHC, and to its employees, regarding the confidentiality of PII and other Protected Information provided to PHC by these providers and PHC employees.

33. PHC required health care provider and employee Class members to furnish their PII, which included, *inter alia*, names, addresses, and Social Security numbers, and banking information, as a condition precedent to credentialing or employment. PHC required the sensitive information to verify their identities, provide agreed-upon compensation and benefits, and for tax purposes, amongst other things.

34. Understanding the sensitive nature of PII, PHC expressly and implicitly promised health care provider and employee Class Members that it would take adequate measures to protect their PII.

---

[2] *Id.*
[3] *Id.*
[4] https://peoplesfamilystl.org/wp-content/uploads/2017/06/Patient-rights-and-responsibilities-PDF-Aug-2012.pdf

35. Indeed, a material term of the contracts between PHC and the health care providers and employees is a covenant by PHC that it will take reasonable efforts to safeguard its confidential PII.

36. Employees of PHC and health care providers wishing to be credentialed by PHC, including Class Members, reasonably relied upon this covenant and would not have disclosed their PII without assurances that it would be properly safeguarded.

37. Moreover, the covenant to adequately safeguard employee and health care provider Class Members' PII is an implied material term of Class Members' employment or credentialing relationship--to the extent that it is not an express material term.

THE RANSOMWARE ATTACK

38. A ransomware attack is a type of malicious software that blocks access to a computer system or data, usually by encrypting it, until the victim pays a fee to the attacker.[5]

39. On September 2, 2019, PHC experienced a cyber-attack from an unknown foreign actor.

40. The incident was discovered on September 3, 2019.

41. A preliminary assessment of this cyber incident determined that there had been improper access to certain portions of PHC's network and computer systems and that a computer "ransomware" virus had encrypted (i.e., made unreadable) certain files on its computer systems.

42. The Ransomware Attack held hostage a critical portion of PHC's computer systems, including patient files and medical records, resulting in service disruptions throughout the organization.

43. As a consequence of the cyber-attack on PHC's computer systems, certain affected data was encrypted and locked away by the ransomware. This data included the Protected Health

[5] https://www.proofpoint.com/us/threat-reference/ransomware.

Information, or PHI (i.e., medical records, demographics, insurance information, medical history, treatment, and billing information), of Defendant PHC's patients, including Plaintiffs and class members, who entrusted Defendant with this highly sensitive and private information.

44. PII of PHC employees and health care providers who sought to be credentialed by PHC was also breached in the attack.

45. Plaintiffs believe their Private Information was stolen (and subsequently sold) in the Ransomware Attack. In the past year, ransomware variants have expanded to include data exfiltration, participation in distributed denial of service (DDoS) attacks, and anti-detection components. One variant deletes files regardless of whether or not a payment was made. Another variant includes the capability to lock cloud-based backups when systems continuously back up in real-time (a.k.a. during persistent synchronization). Other variants target smartphones and Internet of Things (IoT) devices.[6]

46. Defendant admits that it has "no way of knowing whether the information that has been locked in our system has actually been viewed or accessed by this foreign actor," and could not rule out the possibility of unauthorized data access and data exfiltration in the course of its forensic investigation.[7]

47. On or about October 28, 2019, Defendant PHC notified patients, employees, and health care providers of the data security incident that the health system had first become aware of on September 3, 2019.[8]

[6] https://www.cisecurity.org/blog/ransomware-facts-threats-and-countermeasures/

[7] http://phcenters.org/wp-content/uploads/sites/3/2019/10/Notice.pdf

[8] A copy of the notice of data breach may be found here. http://phcenters.org/wp-content/uploads/sites/3/2019/10/Notice.pdf

48. Defendant had obligations created by HIPAA, contract, industry standards, common law, and representations made to Plaintiffs and class members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

49. Plaintiffs and class members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

50. Defendant' data security obligations were particularly important given the substantial increase in ransomware attacks and/or data breaches in the healthcare industry preceding the date of the breach.

51. Indeed, ransomware attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and ***hospitals*** are attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[9]

52. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant PHC.

53. Defendant breached its obligations to Plaintiffs and class members because it failed to properly maintain and safeguard the PHC computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

[9] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (emphasis added).

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

g. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

h. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

i. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

j. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

k. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

l. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b); and/or

m. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption).

54. As the result of computer systems in dire need of security upgrading, inadequate procedures for handling emails containing ransomware or other malignant computer code, and inadequately trained

employees who opened files containing the ransomware virus, Defendant PHC unlawfully failed to safeguard Plaintiffs' and class members' Private Information.

55. Accordingly, as outlined below, Plaintiffs' and class members' daily lives were severely disrupted. What's more, they now face an increased risk of fraud and identity theft.

RANSOMWARE ATTACKS AND DATA BREACHES CAUSE DISRUPTION AND PUT CONSUMERS AT AN INCREASED RISK OF FRAUD AND IDENTIFY THEFT

56. Ransomware attacks at medical facilities such as Defendant PHC's are especially problematic because of the disruption they cause to the medical treatment and overall daily lives of patients affected by the attack.

57. For instance, loss of access to patient histories, charts, images and other information forces providers to limit or cancel patient treatment because of the disruption of service.

58. This leads to a deterioration in the quality of overall care patients receive at facilities affected by ransomware attacks and related data breaches.

59. Researchers have found that at medical facilities that experienced a data security incident, the death rate among patients increased in the months and years after the attack.[10]

60. Researchers have further found that at medical facilities that experienced a data security incident, the incident was associated with deterioration in patient outcomes, generally.[11]

61. Similarly, ransomware attacks and related data security incidents inconvenience patients. Inconveniences patients encounter as a result of such incidents include, but are not limited, to the following:

a. rescheduling medical treatment;

b. finding alternative medical care and treatment;

---

[10] *See* https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks

[11] *See* https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

c. delaying or foregoing medical care and treatment;

d. undergoing medical care and treatment without medical providers having access to a complete medical history and records; and

e. losing patient medical history.[12]

62. Ransomware attacks also constitute data breaches in the traditional sense. For example, in a ransomware advisory, the Department of Health and Human Services informed entities covered by HIPAA that "when electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information)."[13]

63. Ransomware attacks are also considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40[14]

64. Other security experts agree that when ransomware attack occurs, a data breach does as well, because such an attack represents a loss of control of the data within a network.[15]

65. Ransomware attacks are also Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

> The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized

[12] *See, e.g.*, https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/; https://healthitsecurity.com/news/data-breaches-will-cost-healthcare-4b-in-2019-threats-outpace-tech

[13] *See* https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.

[14] *Id.*

[15] *See e.g.*, https://www.csoonline.com/article/3385520/how-hackers-use-ransomware-to-hide-data-breaches-and-other-attacks.html; https://www.varonis.com/blog/is-a-ransomware-attack-a-data-breach/; https://digitalguardian.com/blog/ransomware-infection-always-data-breach-yes.

> access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. See 45 C.F.R.164.308(a)(6).[16]

66. Data breaches represent yet another problem for patients who have already experienced inconvenience and disruption associated with a ransomware attack.

67. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GOA Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[17]

68. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[18]

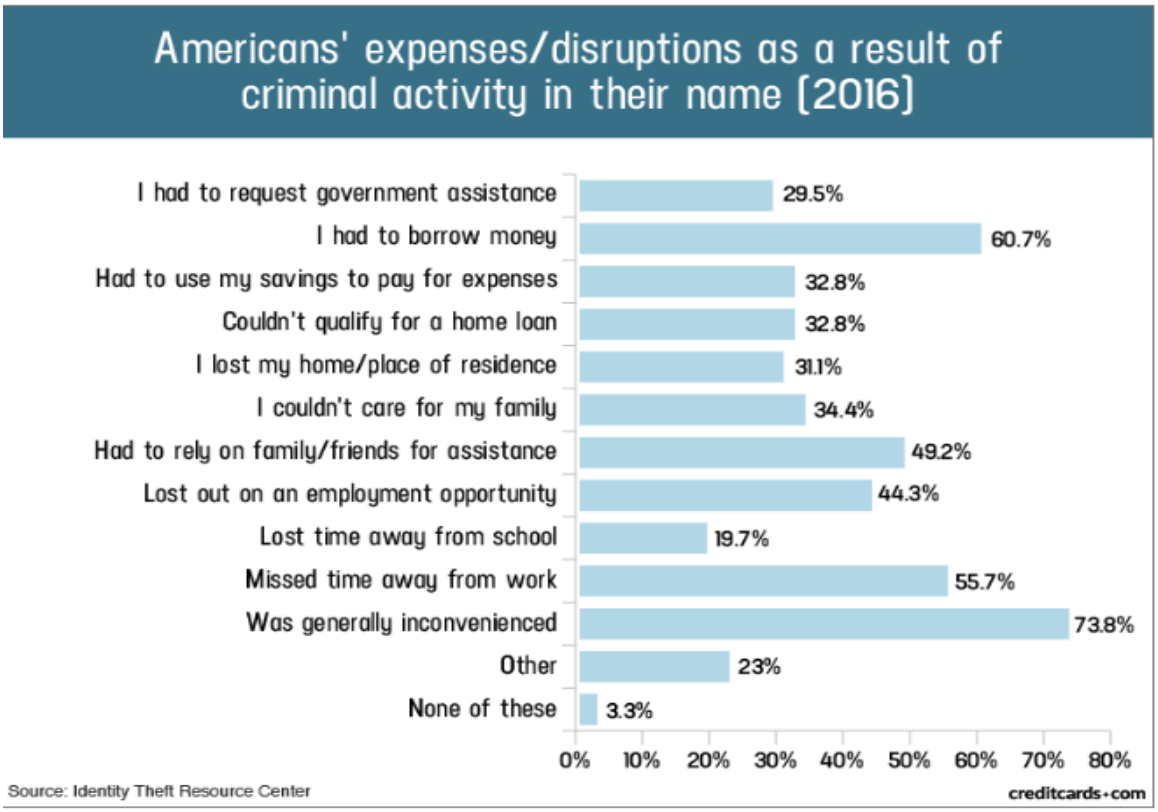
69. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

70. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

---

[16] *See* https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf
[17] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 12, 2019) ("GAO Report").
[18] *See* https://www.identitytheft.gov/Steps (last visited April 12, 2019).

A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[19]



71. What's more, theft of Private Information is also gravely serious. PII/PHI is a valuable property right.[20] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

[19] "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited June 20, 2019).

[20] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

72. Theft of PHI, in particular, is gravely serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[21] Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

73. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

74. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

75. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and Class members are at an increased risk of fraud and identity theft for many years into the future. Thus,

[21] *See* Federal Trade Commission, Medical Identity Theft, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited March 27, 2014).

Plaintiffs and class members must vigilantly monitor their financial and medical accounts for many years to come.

76. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016 – the same as a Facebook account. That pales in comparison with the asking price for medical data, which was selling for $50 and up.[22]

77. Because of its value, the medical industry has experienced disproportionally higher numbers of data theft events than other industries. Defendant therefore knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

PLAINTIFFS' AND CLASS MEMBERS' DAMAGES

78. To date, Defendant has done absolutely nothing to provide Plaintiffs and Class Members with relief for the damages they have suffered as a result of the Ransomware Attack, including, but not limited to, the costs and loss of time they incurred because of the disruption of service at Defendant's medical facilities. Nor has Defendant offered full and effective protection against the likely and probable effects that will result from Plaintiffs' and Class Members' Private Information being stolen in connection with the attack.

79. Plaintiffs and Class members have been damaged by the compromise of their Private Information in the Ransomware Attack.

80. Plaintiff Jerika Barnes Jenkins's Private Information was compromised as a direct and proximate result of the Ransomware Attack.

[22] https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content.

81. Plaintiff Michelle Simmons's Private Information was compromised as a direct and proximate result of the Ransomware Attack.

82. Plaintiff Rayomi Woods's Private Information was compromised as a direct and proximate result of the Ransomware Attack.

83. Plaintiff Kayomi Williams's Private Information was compromised as a direct and proximate result of the Ransomware Attack.

84. Plaintiff L.S.'s Private Information was compromised as a direct and proximate result of the Ransomware Attack,

85. Like Plaintiffs, as a direct and proximate result of Defendant's conduct, Class members had their Protected Information compromised and their medical care and treatment disrupted.

86. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

87. Plaintiffs and Class members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

88. Plaintiffs and Class members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs and class members.

89. Plaintiffs and Class members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Ransomware Attack.

90. Plaintiffs and Class members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Ransomware Attack. Numerous courts have recognized the propriety of loss of value damages in related cases.

91. Class members were also damaged via benefit-of-the-bargain damages. Such class members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Class members paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant PHC's computer property and Plaintiffs' and Class members' Private Information. Thus, Plaintiffs and the Class members did not get what they paid for.

92. Plaintiffs and Class members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse.

93. Plaintiffs and Class members have suffered or will suffer actual injury as a direct result of the Ransomware Attack. In addition to the loss of use of and access to their medical records and costs associated with the inability to access their medical records (including actual disruption of medical care and treatment), many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Ransomware Attack relating to:

a. Finding alternative medical care and treatment;

b. Delaying or foregoing medical care and treatment;

c. Undergoing medical care and treatment without medical providers having access to a complete medical history and records;

d. Having to retrace or recreate their medical history;

e. Finding fraudulent charges;

f. Canceling and reissuing credit and debit cards;

g. Purchasing credit monitoring and identity theft prevention;

h. Addressing their inability to withdraw funds linked to compromised accounts;

i. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

j. Placing "freezes" and "alerts" with credit reporting agencies;

k. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

l. Contacting financial institutions and closing or modifying financial accounts;

m. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

n. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

o. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

94. Moreover, Plaintiffs and Class members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

95. Further, as a result of Defendant's conduct, Plaintiffs and Class members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

96. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

CLASS ACTION ALLEGATIONS

97. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated ("the Class").

98. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> All persons whose Private Information was maintained on Defendant PHC's system that was compromised in the Ransomware Attack discovered on September 3, 2019.

Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

99. Numerosity. The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of approximately 152,000 PHC patients, PHC employees, and health care providers seeking to become credentialed by Defendant PHC whose data was compromised in the Ransomware attack.

100. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Ransomware Attack;

c. Whether Defendant's data security systems prior to and during the Ransomware Attack complied with applicable data security laws and regulations including, *e.g.*, HIPAA;

d. Whether Defendant's data security systems prior to and during the Ransomware Attack were consistent with industry standards;

e. Whether Defendant owed a duty to class members to safeguard their Private Information;

f. Whether Defendant breached their duty to class members to safeguard their Private Information;

g. Whether computer hackers obtained class members' Private Information in the Ransomware attack;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiffs and class members suffered legally cognizable damages as a result of Defendant' misconduct;

j. Whether Plaintiffs and Class members are entitled to damages and/or injunctive relief.

101. Typicality. Plaintiffs' claims are typical of those of other Class members because Plaintiffs' information, like that of every other Class member, was compromised in the Ransomware Attack.

102. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

103. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class members, in that all the Plaintiffs' and Class members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting class members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

104. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most class members would likely find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to individual class

members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each class member.

105. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

CAUSES OF ACTION

FIRST COUNT

Breach of Express Contract
(On Behalf of Plaintiffs and All Class Members)

106. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 105 above as if fully set forth herein.

107. Plaintiffs and members of the Class allege that they entered into valid and enforceable express contracts, or were third party beneficiaries of valid and enforceable express contracts, with Defendant.

108. The valid and enforceable express contracts that Plaintiffs and Class members entered into with Defendant include Defendant's promise to protect nonpublic personal information given to Defendant or that Defendant gathers on its own from disclosure.

109. Under these express contracts, Defendant and/or its affiliated healthcare providers, promised and were obligated to: (a) provide healthcare to Plaintiffs and Class members; and (b) protect Plaintiffs' and the Class members' PII/PHI: (i) provided to obtain such healthcare; and/or (ii) created as a result of providing such healthcare. In exchange, Plaintiffs and members of the Class agreed to pay money for these services, or upheld their employment obligations with PHC, or fulfilled the obligations of their credentialed relationship with PHC, or otherwise fulfilled their contractual obligations with Defendant.

110. Both the provision of healthcare and the protection of Plaintiffs' and Class members' PII/PHI were material aspects of these contracts.

111. At all relevant times, Defendant expressly represented in its Notice of Privacy Practices that it is required by law to (1) maintain "the privacy of your individually identifiable health information ("IIHI")"; (2) notify a patient of a "breach of any of your unsecured Protected Health Information within 60 days"; (3) "provide you with this notice of our legal duties and the privacy practices that we maintain in our Health Center concerning your IIHI"; (4) abide by the legal requirement "to maintain the confidentiality of health information that identifies you," and; 5) follow the terms of the Notice of Privacy Practices that PHC has in effect at the time.

112. Defendant's express representations, including, but not limited to, express representations found in its Notice of Privacy Practices, formed an express contract requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class members' PII/PHI.

113. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their PII/PHI associated with obtaining healthcare private. To customers such as Plaintiffs and Class members, healthcare that does not adhere to industry standard data security protocols to protect PII/PHI is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security. Plaintiffs and Class members would not have entered into these contracts with Defendant and/or its affiliated healthcare providers as a direct or third-party beneficiary without an understanding that their PII/PHI would be safeguarded and protected.

114. A meeting of the minds occurred, as Plaintiffs and members of the Class provided their PII/PHI to Defendant and/or its affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, protection of their PII/PHI.

115. Employee class members provided PII to Defendant and performed their contractual employment obligations in exchange for, amongst other things, protection of their PII.

116. Health care provider class members provided PII to Defendant and performed their contractual obligations under the credentialing arrangement in exchange for, amongst other things, protection of their PII.

117. Plaintiffs and Class members performed their obligations under the contract when they paid for their health care services, when they performed their employment obligations, when they fulfilled their obligations under the credentialing agreements, or otherwise fulfilled their contractual obligations with Defendant.

118. Defendant materially breached its contractual obligations to protect the nonpublic personal information Defendant gathered when the information was accessed and exfiltrated by unauthorized personnel as part of the Ransomware Attack.

119. Defendant materially breached the terms of these express contracts, including, but not limited to, the terms stated in the relevant Notice of Privacy Practices. Defendant did not "maintain the privacy" of Plaintiffs' and Class members' PII/PHI as evidenced by its notifications of the Ransomware Attack to Plaintiffs and 152,000 Class members. Specifically, Defendant did not comply with industry standards, or otherwise protect Plaintiffs' and the Class members' PII/PHI, as set forth above.

120. The Ransomware Attack was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

121. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiffs and members of the Class did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiffs and Class members therefore were damaged in an amount at least equal to the

difference in the value of the healthcare with data security protection they paid for and the healthcare they received.

122. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiffs, the Class members, nor any reasonable person would have purchased healthcare from Defendant and/or its affiliated healthcare providers.

123. As a direct and proximate result of the data security incident, Plaintiffs and Class members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure, and publication of their PII/PHI, the loss of control of their PII/PHI, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

124. Plaintiffs and Class members are entitled to compensatory and consequential damages suffered as a result of the Ransomware Attack.

SECOND COUNT

Breach of Implied Contract
(On Behalf of Plaintiffs and All Class Members)

125. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 105 above as if fully set forth herein.

126. When Plaintiffs and Class members provided their Private Information to Defendant PHC in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

127. Defendant solicited and invited class members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class members accepted Defendant's offers and provided their Private Information to Defendant.

128. In entering into such implied contracts, Plaintiffs and Class members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

129. Class members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

130. Plaintiffs and Class members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiffs and Class members would not have entrusted their Private Information to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that Defendant adopted reasonable data security measures.

131. Plaintiffs and Class members fully and adequately performed their obligations under the implied contracts with Defendant.

132. Defendant breached its implied contracts with Class members by failing to safeguard and protect their Private Information.

133. As a direct and proximate result of Defendant's breaches of the implied contracts, Class members sustained damages as alleged herein.

134. Plaintiffs and Class members are entitled to compensatory and consequential damages suffered as a result of the Ransomware Attack.

135. Plaintiffs and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class members.

THIRD COUNT

VIOLATIONS OF THE MISSOURI MERCHANDISING PRACTICES ACT ("MMPA"), MISSOURI REVISED STATUTES CHAPTER 407 (RSMo) (On Behalf of Plaintiffs and All Class Members)

136. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 105 above as if fully set forth herein.

137. Plaintiffs and Class members are consumers who made payments to Defendant for merchandise (consisting of medical services) that were primarily for personal, family, or household purposes.

138. Defendant engaged in the conduct alleged in this Complaint, entering into transactions intended to result, and which did result, in the sale of merchandise (consisting of medical services) to consumers, including Plaintiffs and Class members.

139. Defendants engaged in, and its acts and omissions affect, trade and commerce.

140. Defendants' acts, practices, and omissions were done in the course of Defendants' business of marketing, offering to sell, and selling merchandise (consisting of medical services) to consumers in the State of Missouri.

141. Defendant, operating in Missouri, engaged in deceptive, unfair and unlawful practices in connection with the sale or advertisement of merchandise (consisting of medical services) as defined by MO Rev Stat. § 407.020, including but not limited to the following:

a. failure to maintain adequate computer systems and data security practices to safeguard Private Information;

b. failure to disclose that its computer systems and data security practices were inadequate to safeguard Private Information from theft;

c. continued gathering and storage of PHI, PII, and other personal information after Defendant knew or should have known of the security vulnerabilities of its computer systems that were exploited in the Ransomware Attack;

d. making and using false promises, set out in the PHC Privacy Notice and Patients' Rights and Responsibilities, about the privacy and security of PHI, PII, and the Private Information of Plaintiffs and Class Members, and;

e. continued gathering and storage of PHI, PII, and other personal information after Defendant knew or should have known of the Ransomware Attack and before Defendant allegedly remediated the data security incident.

142. These unfair acts and practices violated duties imposed by laws, including but not limited to the Federal Trade Commission Act, HIPAA, the Gramm- Leach-Bliley Act, and the MMPA (MO Rev. Stat. § 407.020).

143. As a direct and proximate result of Defendant's violation of the MMPA, Plaintiffs and the Class members suffered damages including, but not limited to: (i) actual disruption of ongoing medical care and treatment; (ii) actual identity theft; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Ransomware Attack, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vii) future costs in terms of time, effort, and money that will be expended as result of the Ransomware Attack for the remainder

of the lives of Plaintiffs and Class Members; and (viii) the diminished value of Defendant's services they received.

144. Also as a direct result of Defendant's violation of the MMPA, Plaintiffs and the Class members are entitled to damages as well as injunctive relief, including, but not limited to, ordering Defendants to: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class members.

145. Plaintiffs bring this action on behalf of themselves and Class members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiffs, Class members and the public from Defendant's unfair, deceptive, and unlawful practices. Defendant's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

146. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Class members' Private Information and that the risk of a data security incident was high.

147. Plaintiffs and Class members seek relief under the MMPA including, but not limited to, actual damages, injunctive or other equitable relief, punitive damages, and reasonable attorney's fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiffs and their Counsel to represent the Class;

b) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII and PHI compromised during the Ransomware Attack;

c) Ordering Defendant to pay for not less than five (5) years of credit monitoring services for Plaintiffs and the Class;

d) For an award of actual damages, compensatory damages, punitive damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

e) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

f) Pre- and post-judgment interest on any amounts awarded; and

g) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiffs demand a jury trial on all issues so triable.

Dated: January 7, 2020

Respectfully submitted,

/s/ Brandon M. Wise
Brandon M. Wise – Mo. Bar #67242
Paul A. Lesko – Mo. Bar #51914
PEIFFER WOLF CARR & KANE, APLC
818 Lafayette Ave., Floor 2
St. Louis, MO 63104
Phone: 314.833.4825
bwise@pwcklegal.com
plesko@pwcklegal.com

Gary E. Mason (*pro hac vice forthcoming*)
WHITFIELD BRYSON & MASON LLP
5101 Wisconsin Ave., NW, Ste. 305
Washington, DC 20016
Phone: 202.640.1160
Fax: 202.429.2294
gmason@wbmllp.com

Gary M. Klinger (*pro hac vice forthcoming*)
KOZONIS & KLINGER, LTD.
227 W. Monroe Street, Suite 2100
Chicago, Illinois 60630
Phone: 312.283.3814
Fax: 773.496.8617
gklinger@kozonislaw.com

ATTORNEYS FOR PLAINTIFFS AND
THE PROPOSED CLASS